

Detection of malicious data in vehicular ad-hoc networks for traffic signal control applications

Bartłomiej Płaczek and Marcin Bernas

University of Silesia, Institute of Computer Science,
Będzińska 39, 41-200 Sosnowiec, Poland
{placzek.bartlomiej,marcin.bernas}@gmail.com

Abstract. Effective applications of vehicular ad hoc networks in traffic signal control require new methods for detection of malicious data. Injection of malicious data can result in significantly decreased performance of such applications, increased vehicle delays, fuel consumption, congestion, or even safety threats. This paper introduces a method, which combines a model of expected driver behaviour with position verification in order to detect the malicious data injected by vehicle nodes that perform Sybil attacks. Effectiveness of this approach was demonstrated in simulation experiments for a decentralized self-organizing system that controls the traffic signals at multiple intersections in an urban road network. Experimental results show that the proposed method is useful for mitigating the negative impact of malicious data on the performance of traffic signal control.¹

Keywords: vehicular networks, malicious data, Sybil attack, traffic signal control

1 Introduction

Vehicular ad-hoc networks (VANETs) facilitate wireless data transfer between vehicles and infrastructure. The vehicles in VANET can provide detailed and useful data including their positions, velocities, and accelerations. This technology opens new perspectives in traffic signal control and creates an opportunity to overcome main limitations of the existing roadside sensors, i.e., low coverage, local measurements, high installation and maintenance costs. The availability of the detailed data from vehicles results in a higher performance of the traffic signal control [1,2,3].

The VANET-based traffic signal systems have gained considerable interest in recent years. In this field the various solutions have been proposed that extend existing adaptive signal systems for isolated intersections [4,5]. For such systems

¹ Preprint of: Płaczek, B., Bernas, M.: Detection of malicious data in vehicular ad-hoc networks for traffic signal control applications. in Gaj, P., Kwiecien, A., Stera, P. (eds.) Computer Networks. CCIS, vol. 608, pp. 72-82, 2016. The final publication is available at link.springer.com

the data collected in VANET are used to estimate queue lengths and vehicle delays. On this basis optimal cycle length and split of signal phases are calculated. Similar adaptive approach was also used to control traffic signals at multiple intersections in a road network [6,7]. Particularly advantageous for VANET-based systems is the self-organizing signal control scheme, which enables a decentralized optimization, global coordination of the traffic streams in a road network, and improved performance [8].

Effective VANET applications in traffic signal control require new methods for real-time detection of attacks that are based on malicious data. Injection of malicious data can result in significantly decreased performance of the traffic signal control, increased vehicle delays, fuel consumption, congestion, or even safety threats.

This paper introduces a method for the above mentioned applications, which can be used to detect malicious data. The considered malicious data are injected by vehicle nodes that perform Sybil attacks, i.e., create a large number of false vehicle nodes in order to influence the operation of traffic signals. The proposed method detects the malicious data by combining a model of expected driver behaviour with a position verification approach.

The paper is organized as follows. Related works are discussed in Section 2. Section 3 introduces the proposed method. Results of simulation experiments are presented in Section 4. Finally, conclusions are given in Section 5.

2 Related works

The problem of malicious nodes detection in VANETs has received particular attention and various methods have been proposed so far [9]. The existing solutions can be categorized into three main classes: encryption and authentication methods, methods based on position verification, and methods based on VANET modelling.

In the encryption and authentication methods, malicious nodes detection is implemented by using authentication mechanisms. One of the approaches is to authenticate vehicles via public key cryptography [10]. The methods that use public key infrastructure were discussed in [11]. Main disadvantages of such methods are difficulties in accessing to the network infrastructure and long computational time of encryption and digital signature processing. Public key encryption and message authentication systems consume time and memory. Thus, bandwidth and resource consumption is increased in the public key systems.

In [12] an authentication scheme was proposed, which assumes that vehicles collect certified time stamps from roadside units as they are travelling. The malicious nodes detection is based on verification of the collected series of time stamps. Another similar method [13] assumes that vehicles receive temporary certificates from roadside units and malicious nodes detection is performed by checking spatial and temporal correlation between vehicles and roadside units. These methods require a dense deployment of the roadside units.

Position verification methods are based on the fact that position reported by a vehicle can be verified by other vehicles or by roadside units [14]. The key requirement in this category of the methods is accurate position information. A popular approach is to detect inconsistencies between the strength of received signal and the claimed vehicle position by using a propagation model. According to the method introduced in [15] signal strength measurements are collected when nodes send beacon messages. The collected measurements are used to estimate position of the nodes according to a given propagation model. A node is considered to be malicious if its claimed position is too far from the estimated one. In [16] methods were proposed for determining a transmitting node location by using signal properties and trusted peers collaboration for identification and authentication purposes. That method utilizes signal strength and direction measurements thus it requires application of directional antennas.

Xiao et al. [17] and Yu et al. [18] proposed a distributed method for detection and localization of malicious nodes in VANET by using verifier nodes that confirm claimed position of each vehicle. In this approach, statistical analysis of received signal strength is performed by neighbouring vehicles over a period of time in order to calculate the position of a claimer vehicle. Each vehicle has the role of claimer, witness, or verifier on different occasions and for different purposes. The claimer vehicle periodically broadcasts its location and identity information, and then, verifier vehicle confirms the claimer position by using a set of witness vehicles. Traffic pattern analysis and support of roadside units is used for selection of the witness vehicles. Yan et al. [19] proposed an approach that uses on-board radar to detect neighbouring vehicles and verify their positions.

The modelling-based methods utilize models that describe expected behaviour of vehicle nodes in VANET. These methods detect malicious nodes by comparing the model with information collected from the vehicles. Golle et al. [20] proposed a general model-based approach to evaluating the validity of data collected from vehicle nodes. According to this approach, different explanations for the received data are searched by taking into account the possible presence of malicious nodes. Explanations that are consistent with a model of the VANET get scores. The node accepts data that are consistent with the most scored explanation. On this basis, the nodes can detect malicious data and identify the vehicles that are the sources of such data. Another method in this category relies on comparing the behaviour of a vehicle with a model of average driving behaviour, which is built on the fly by using data collected from other vehicles [21].

In [22] a malicious data detection scheme was proposed for post crash notification applications that broadcast warnings to approaching traffic. A vehicle node observes driver's behaviour for some time after the warning is received and compares it with some expected behaviour. The vehicle movement in the absence of any traffic accident is assumed to follow some free-flow mobility model, and its movement in case of accident is assumed to follow some crash-modulated mobility model. On this basis the node can decide if the received warning is true or false.

A framework based on subjective logic was introduced in [23] for malicious data detection in vehicle-to-infrastructure communication. According to that approach, all data collected by a vehicle node can be mapped to a world-model and can then be annotated with opinions by different misbehaviour detection mechanisms. The opinions are used not only to express belief or disbelief in a stated fact or data source, but also to model uncertainty. Authors have shown that application of the subjective logic operators, such as consensus or transitivity, allows different misbehaviour detection mechanisms to be effectively combined.

According to the authors' knowledge, the problem of malicious data detection for traffic signal control applications has not been studied so far in VANET-related literature. In this paper a malicious data detection method is introduced for VANET-based traffic signal control systems. The proposed method integrates a model of expected driver behaviour with position verification in order to detect the malicious data that can degrade the performance of road traffic control at signalized intersections.

3 Proposed method

This section introduces an approach, which was intended to detect malicious data in VANET applications for road traffic control at signalized intersections. The considered VANET is composed of vehicle nodes and control nodes that manage traffic signals at intersections. Vehicles are equipped with sensors that collect speed and position data. The collected information is periodically transmitted from vehicles to control nodes. The control nodes use this information for optimizing traffic signals to decrease delay of vehicles and increase capacity of a road network.

In order to detect and filter out malicious data, the control node assigns a trust level to each reported vehicle. The trust levels are updated (decreased or increased) after each data delivery by using the rules discussed later in this section. When making decisions related to changes of traffic signals, the control node takes into account only those data that were collected by vehicles with positive trust level. The data delivered by vehicles with trust level below or equal to zero are recognized as malicious and ignored.

At each time step vehicle reports ID of its current traffic lane, its position along the lane, and velocity. If vehicles i and j are moving in the same lane during some time period and at the beginning of this period vehicle i is in front of vehicle j then the same order of vehicles has to be observed for the entire period. Thus, the following rule is used to detect the unrealistic behaviour of vehicles in a single lane:

$$x_i(t) - x_j(t) > \epsilon_x \wedge x_i(t - \delta) - x_j(t - \delta) < -\epsilon_x \wedge l_i(t') = l_j(t') \quad \forall t' : t - \delta \leq t' \leq t, \quad (1)$$

where: $l_i(t)$, $x_i(t)$, $v_i(t)$ denote respectively lane ID, position, and velocity of vehicle i at time step t , δ is length of the time period, and ϵ_x is maximum localization error. It is assumed that the frequency of data reports enables recognition of overtaking. In situation when condition (1) is satisfied and both vehicles have

positive trust level, the trust level of both vehicles (i and j) is decreased by value α because the collected data do not allow us to recognize which one of the two reported vehicles is malicious. If one of the two vehicles has non-positive trust level then the trust level is decreased only for this vehicle.

According to the second rule (so-called reaction to signal rule), current traffic signals are taken into account in order to recognize the malicious data. If the information received from vehicle i indicates that this vehicle enters an intersection when red signal is displayed or stops at green signal then the trust level of vehicle i is decreased by value α . The following condition is used to detect the vehicles passing at red signal:

$$h_n - x_j(t - \delta) > \epsilon_x \wedge h_n - x_j(t) < -\epsilon_x \wedge s_n(t') = \text{red} \quad \forall t' : t - \delta \leq t' \leq t, \quad (2)$$

where: h_n is position of the stop line for signal n , $s_n(t)$ is the colour of signal n at time t , and the remaining symbols are identical to those defined for rule (1). The vehicles stopped at green signal are recognized according to condition:

$$|h_n - x_j(t')| < \epsilon_x \quad \forall t' : t - \delta \leq t' \leq t \wedge s_n(t') = \text{green} \quad \forall t' : t - \delta \leq t' \leq t, \quad (3)$$

where $|\cdot|$ denotes absolute value and the remaining symbols were defined above. In opposite situations, when the vehicle enters the intersection during green signal or stops at red signal then its trust level is increased by α .

Theoretical models of vehicular traffic assume that vehicles move with desired free flow velocity if they are not affected by other vehicles or traffic signals [24]. Based on this assumption, expected velocity of vehicle i can be estimated as follows:

$$\hat{v}_i(t) = \min \left(v_f, \frac{h_i(t) - h_{\min}}{\tau} \right), \quad (4)$$

where: v_f is free flow velocity, $h_i(t)$ is headway distance, i.e., distance between vehicle i and vehicle in front in the same lane or distance between vehicle i and the nearest red signal, h_{\min} is minimum required headway distance for stopped vehicle, τ denotes time which is necessary to stop vehicle safely and leave adequate space from the preceding car or traffic signal. Time τ can be determined according to the two seconds rule, which is suggested by road safety authorities [25].

When the velocity reported by a vehicle differs significantly from the expected velocity then the vehicle is suspected to be malicious. Thus, the trust level of the vehicle is decreased. In opposite situation, when the reported velocity is close to the expected value, the trust level is increased. According to the above assumptions, the trust level is updated by adding value $u_i(t) \cdot \beta$ and $u_i(t)$ is calculated using the following formula:

$$u_i(t) = \begin{cases} 1, & |\hat{v}_i(t) - v_i(t)| < \epsilon_v, \\ -\frac{|\hat{v}_i(t) - v_i(t)|}{v_f}, & \text{else,} \end{cases} \quad (5)$$

where ϵ_v is a threshold of the velocity difference, and the remaining symbols were defined earlier. Threshold ϵ_v was introduced in Eq. (5) to take into account error of velocity measurement and uncertainty of the expected velocity determination.

The last rule for updating trust level assumes that vehicles are equipped with sensors which enable detection and localization of neighbouring vehicles within distance r . In this case each vehicle reports the information about its own position and speed as well as positions of other vehicles in the neighbourhood. The information about neighbouring vehicles, delivered by vehicle j at time t , is represented by set $D_j(t)$:

$$D_j(t) = \{\langle x_k(t), l_k(t) \rangle\}, \quad (6)$$

where $x_k(t)$ and $l_k(t)$ denote position and lane of k -th vehicle in the neighbourhood. The additional data can be utilized by control node for verification of the collected vehicle positions. Position of vehicle i should correspond to one of the positions of neighbours (k) reported by vehicle j if distance between vehicles i and j is not greater than r . Therefore, trust level of vehicle i is increased by α if

$$\text{dist}(i, j) \leq r \wedge \exists \langle x_k(t), l_k(t) \rangle \in D_j(t) : \text{dist}(i, k) \leq \epsilon_x, \quad (7)$$

where: $\text{dist}(i, j)$ is distance between vehicles i and j , r is localization range, and the remaining symbols were defined earlier. The trust level is decreased by α if

$$\text{dist}(i, j) \leq r \wedge \text{dist}(i, k) > \epsilon_x \forall \langle x_k(t), l_k(t) \rangle \in D_j(t). \quad (8)$$

The symbols in (8) were defined earlier in this section. The above rule is applied only if the trust level of vehicle j is positive.

It should be noted that the parameter of decreasing trust level for the velocity-related rule (β) is different than for the remaining rules (α) because the velocity-related rule can be used after each data transfer, i.e., significantly more frequently than the other rules.

4 Experiments

Simulation experiments were performed to evaluate effectiveness of the proposed method for malicious data detection. The experimental results presented in this section concern percentages of detected malicious data and the impact of these data on vehicle delay at signalized intersections in a road network.

In this study the stochastic cellular automata model of road network, proposed by Brockfeld et al. [26], was used for the traffic simulation. This model represents a road network in a Manhattan-like city. Topology of the simulated network is a square lattice of 8 unidirectional roads with 16 signalized intersections (Fig. 1). The distance between intersections is of 300 m. Each link in the network is represented by a one-dimensional cellular automaton. An occupied cell on the cellular automaton symbolizes a single vehicle. At each discrete time step (1 second) the state of cellular automata is updated according to four steps (acceleration, braking due to other vehicles or traffic light, velocity randomization, and movement). These steps are necessary to reproduce the basic features of real traffic flow. Step 1 represents driver tendency to drive as fast as possible,

step 2 is necessary to avoid collisions and step 3 introduces random perturbations necessary to take into account changes of vehicle velocity in regions with high density. Finally, in step 4 the vehicles are moved according to the new velocity calculated in steps 1-3. Steps 1-4 are applied in parallel for all vehicles. Detailed definitions of these steps can be found in [26]. Maximum velocity was set to 2 cells per second (54 km/h).

Deceleration probability p for the Brockfeld model is 0.15. The saturation flow at intersections is 1700 vehicles per hour of green time. This model was applied to calculate the stop delay of vehicles. The traffic signals were controlled by using the self-organizing method based on priorities that correspond to "pressures" induced by vehicles waiting at an intersection [27]. The traffic signal control was simulated assuming the intergreen times of 5 s and the maximum period of 120 s. At each intersection there are two alternative control actions: the green signal can be given to vehicles coming from south or to those that are coming from west. The simulator was implemented in Matlab.

Intensity of the traffic flow is determined for the network model by parameter q in vehicles per second. This parameter refers to all traffic streams entering the road network. At each time step vehicles are randomly generated with a probability equal to the intensity q in all traffic lanes of the network model. Similarly, the false (malicious) vehicles are generated with intensity q_F at random locations. The false vehicles move with constant, randomly selected velocity.

During experiments nine algorithms of malicious data detection were taken into account (Tab. 1). The algorithms use different combinations of the rules proposed in Sect. 3 (4 rules used separately and 5 selected combinations that achieved the most promising results in preliminary tests). Simulations were performed for four various intensities of true vehicles ($q = 0.02, 0.06, 0.10, 0.14$) and false vehicles ($q_F = 0.02, 0.04, 0.06, 0.08$). For each combination of the intensities q and q_F the simulation was executed in 20 runs of 10 minutes. Based on preliminary results, the parameters used for updating the trust levels were set as follows: $\alpha = 1$ and $\beta = 0.2$.

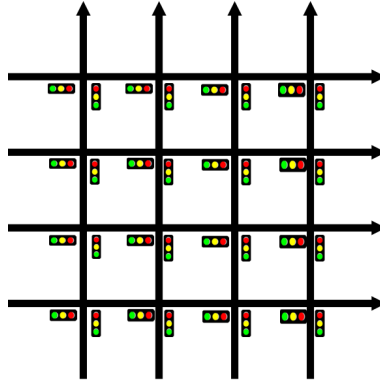


Fig. 1. Simulated road network

Table 1. Compared algorithms for malicious data detection

Algorithm	Rule	1	2	3	4	5	6	7	8	9
1 - vehicles order		+	-	-	-	+	-	+	-	+
2 - reaction to signals		-	-	+	-	+	+	-	-	+
3 - expected velocity		-	-	-	+	-	-	+	+	+
4 - neighbour detection		-	+	-	-	-	+	-	+	+

Figure 2 shows percentages of correctly detected malicious data and correctly recognized true data for two different intensities of false vehicles. The data were categorized as true or malicious at each one-second interval.

Total delay of vehicles for the considered algorithms is compared in Fig. 3. The results in Fig. 3 were averaged for all considered true and false vehicle intensities. Average number of vehicles for one simulation run (10 minutes) was 384. The best results were obtained for algorithm 9, which utilizes all proposed rules for detection of the malicious data. This algorithm allows the delay of vehicles to be kept at the low level (close to the value obtained for simulation without malicious data). The delay is increased only by 1% in comparison to the delay observed when no malicious data are present. Algorithm 9 correctly recognizes 90% of the malicious data and 96% of the true data on average. High accuracy was also observed for Algorithm 2, which uses the approach of position verification by neighbouring vehicles without any additional rules. The least satisfactory results were obtained when using the vehicles order rule (Algorithm 1) or the reaction to signals rule (Algorithm 3). For these algorithms the delay of vehicles is close to that observed when the detection of malicious data is not used.

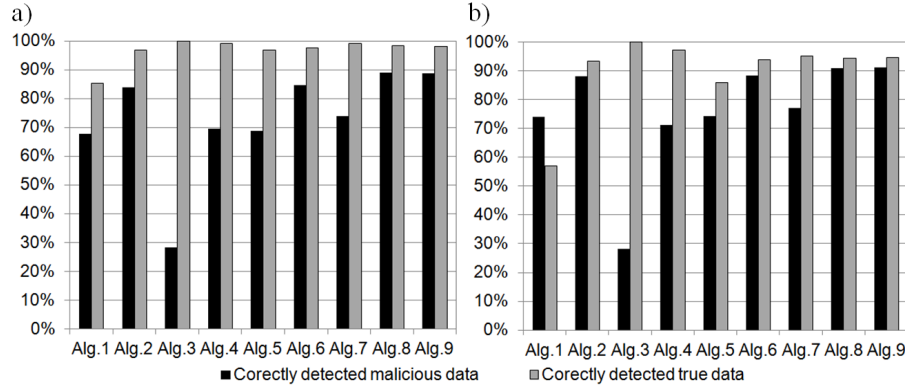


Fig. 2. Accuracy of malicious data detection for the compared algorithms: a) $q_F = 0.02$ veh./s, b) $q_F = 0.08$ veh./s

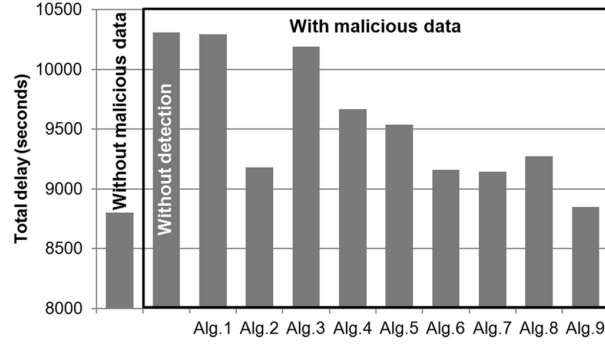


Fig. 3. Average delay of vehicles for the compared algorithms

Figure 4 shows mean vehicle delays for various intensities of the traffic flow (q) and two different intensities of the false vehicles generation (q_F). Algorithm 0 in Fig. 4 corresponds to the situation when no malicious data detection is implemented. It can be observed in these results that the effectiveness of a particular algorithm strongly depends on the considered intensities. For instance, in case of $q = 0.14$ and $q_F = 0.02$ Algorithm 8 causes a higher delay than those obtained without malicious data detection, while for the remaining intensities Algorithm 8 gives good results. However, for Algorithm 9 the delay is reduced when comparing with those obtained without malicious data detection for all considered intensity settings. This fact confirms that all the proposed rules are useful as they contribute with different degree in various traffic conditions to mitigating the negative impact of malicious data.

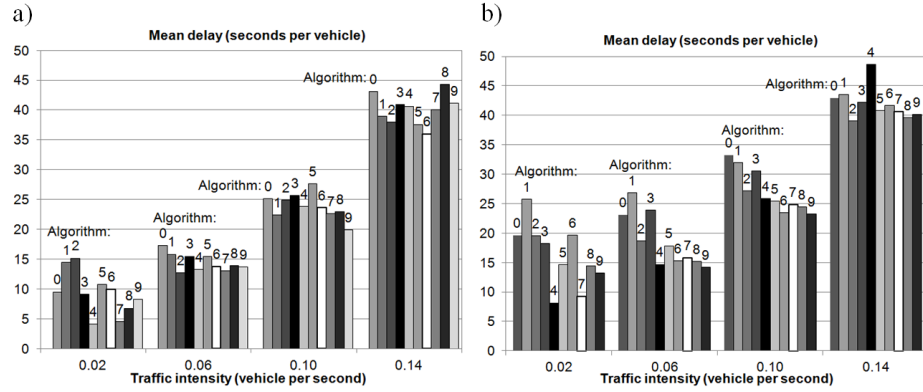


Fig. 4. Mean delay for different traffic intensities: a) $q_F = 0.02$ veh./s, b) $q_F = 0.08$ veh./s

5 Conclusion

Sybil attacks can degrade the performance of VANET-based traffic signal control. The proposed approach enables effective detection of malicious data created in VANETs when the Sybil attacks are launched. The introduced detection scheme is based on rules that take into account unrealistic overtaking manoeuvres, expected driver behaviour (reaction to traffic signals and preferred velocity) as well as verification of vehicle position by neighbouring nodes. Effectiveness of this approach was demonstrated in simulation experiments for a decentralized self-organizing system that controls the traffic signals at multiple intersections in an urban road network. The experimental results show that combination of different detection mechanisms allows the malicious data in VANET to be correctly recognized and is essential for mitigating their negative impact on the performance of traffic signal control. Further research is necessary to integrate the method with more sophisticated models of driver behaviours, enable automatic parameters calibration based on collected data, and test the proposed approach in different (more realistic) scenarios with various traffic control algorithms.

References

1. Bajwa, E. J. S., Walia, E. L.: A Survey on Traffic Management Systems in VANET. *International Journal of Advanced Trends in Computer Applications*, vol. 1, no. 4, pp. 28–32 (2015)
2. Płaczek, B.: Efficient data collection for self-organising traffic signal systems based on vehicular sensor networks. *International Journal of Ad Hoc and Ubiquitous Computing*, in press
3. Płaczek, B.: A self-organizing system for urban traffic control based on predictive interval microscopic model. *Engineering Applications of Artificial Intelligence*, 34, pp. 75–84 (2014)
4. Chang, H. J., Park, G. T.: A study on traffic signal control at signalized intersections in vehicular ad hoc networks, *Ad Hoc Networks* 11, pp. 2115–2124 (2013)
5. Kwatirayo, S., Almhana, J., Liu, Z.: Adaptive Traffic Light Control using VANET: A case study in Wireless Communications and Mobile Computing Conference (IWCMC), IEEE, pp. 752–757 (2013)
6. Maslekar, N., Mouzna, J., Boussedjra, M., Labiod, H.: CATS: An adaptive traffic signal system based on car-to-car communication, *Journal of Network and Computer Applications* 36(5), pp. 1308–1315 (2013)
7. Priemer, C., Friedrich, B.: A decentralized adaptive traffic signal control using V2I communication data in 12th International IEEE Conference on Intelligent Transportation Systems ITSC '09, IEEE, pp. 1–6 (2009)
8. Zhang, L., Garoni, T. M., de Gier, J.: A comparative study of Macroscopic Fundamental Diagrams of arterial road networks governed by adaptive traffic signal systems, *Transportation Research Part B: Methodological* 49, pp. 1–23 (2013)
9. Ali Mohammadi, M., Pouyan, A. A.: Defense mechanisms against Sybil attack in vehicular ad hoc network. *Security and Communication Networks*, 8(6), pp. 917–936 (2015)
10. Bouassida, M.S., Guette, G., Shawky, M., Ducourthial, B.: Sybil nodes detection based on received signal strength variations within VANET. *International Journal of Network Security* 9(1), pp. 22–32 (2009)

11. Raya, M., Papadimitratos, P., Hubaux, J.P.: Securing vehicular communications. *IEEE Wireless Communications Magazine*, Special Issue on Inter-Vehicular Communications 13(5) pp. 8–15 (2006)
12. Chang, S., Qi, Y., Zhu, H., Zhao, J., Shen, X.: Footprint: detecting Sybil attacks in urban vehicular networks. *IEEE Transactions on Parallel and Distributed Systems* 23(6), pp. 1103–1114 (2012)
13. Park, S., Aslam, B., Turgut, D., Zou, C.C.: Defense against Sybil attack in the initial deployment stage of vehicular ad hoc network based on roadside unit support. *Security and Communication Networks* 6(4), pp. 523–538 (2013)
14. Guette, G., Ducourthial, B.: On the Sybil attack detection in VANET. In *Mobile Adhoc and Sensor Systems, MASS 2007. IEEE International Conference on*, pp. 1–6 (2007)
15. Xiao, B., Yu, B., Gao, C.: Detection and localization of sybil nodes in VANETs. In *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 1–8, ACM (2006)
16. Suen, T., Yasinsac, A.: Ad hoc network security: Peer identification and authentication using signal properties. In *Information Assurance Workshop, 2005. IAW'05. Proceedings from the Sixth Annual IEEE SMC*, pp. 432–433 (2005)
17. Xiao, B., Yu, B., Gao, C.: Detection and localization of Sybil nodes in VANETs. *Proceedings of the 2006 workshop on Dependability issues in wireless ad hoc networks and sensor networks*, pp. 1–8 (2006)
18. Yu, B., Xu, C.Z., Xiao, B.: Detecting Sybil attacks in VANETs. *Journal of Parallel and Distributed Computing* 73(6), pp. 746–756 (2013)
19. Yan, G., Olariu, S., Weigle, M.C.: Providing VANET security through active position detection. *Computer Communications* 31(12), pp. 2883–2897 (2008)
20. Golle, P., Greene, D., Staddon, J.: Detecting and correcting malicious data in VANETs. In *Proceedings of the 1st ACM international workshop on Vehicular ad hoc networks*, pp. 29–37, ACM (2004)
21. Raya, M., Papadimitratos, P., Aad, I., Jungels, D., Hubaux, J. P.: Eviction of misbehaving and faulty nodes in vehicular networks. *Selected Areas in Communications, IEEE Journal on*, 25(8), pp. 1557–1568 (2007)
22. Ghosh, M., Varghese, A., Gupta, A., Kherani, A. A., Muthaiah, S. N.: Detecting misbehaviors in VANET with integrated root-cause analysis. *Ad Hoc Networks*, 8(7), pp. 778–790 (2010)
23. Dietzel, S., van der Heijden, R., Decke, H., Kargl, F.: A flexible, subjective logic-based framework for misbehavior detection in V2V networks. In *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), 2014 IEEE 15th International Symposium on*, pp. 1–6, IEEE, (2014)
24. PĄcacek, B.: A Traffic Model Based on Fuzzy Cellular Automata. *Journal of Cellular Automata*, 8(3-4), pp. 261–282 (2013)
25. Thammakaroon, P., Tangamchit, P.: Adaptive brake warning system for automobiles. In *ITS Telecommunications, 2008. ITST 2008. 8th International Conference on*, pp. 204–208, IEEE (2008)
26. Brockfeld, E., Barlovic, R., Schadschneider, A., Schreckenberg, M.: Optimizing traffic lights in a cellular automaton model for city traffic. *Physical Review E*, 64(5), 056132, (2001)
27. Helbing, D., Lämmer, S. and Lebacque, J.P.: Self-organized control of irregular or perturbed network traffic, in: *Optimal Control and Dynamic Games*, Springer US, pp. 239–274 (2005)